eHealth Ontario
www.ehealthontario.on.ca

Ontario
eHealth Ontario

Solution administrative et frontale combinée de ConnexionRGT

Évaluation de l'impact sur la protection de la vie privée

(Résumé et conclusion)

Bureau de la protection de la vie privée

Identificateur du document : S. o.

Version : 1.4

Propriétaire : Réseau universitaire de santé

Résumé

Le programme ConnexionRGT (cRGT) est une initiative de partage d'information sur la santé qui profitera aux patients et aux fournisseurs de soins de santé dans la région centrale l'Ontario. Cette région compte environ 750 fournisseurs de soins de santé, qui desservent une population de 6,75 millions d'habitants (soit 51 % de la population de la province). Les fournisseurs de soins de santé doivent surmonter des obstacles importants pour être en mesure d'échanger les renseignements sur la santé des patients (RSP) qui les aident à administrer leurs traitements en temps utile et de manière efficace. Leurs difficultés sont attribuables à l'existence de divers systèmes d'information déjà en place et à des capacités d'intégration restreintes. Ils s'en tiennent donc souvent à l'information propre à leur organisme ou leur cabinet, ce qui peut limiter la qualité des soins que les cliniciens prodiguent à leurs patients.

Le programme cRGT fonctionne en partenariat avec six réseaux locaux d'intégration des services de santé (RLISS) de la région centrale de l'Ontario : les RLISS du Centre, du Centre-Est, du Centre-Ouest, de Mississauga Halton, de Centre-Toronto et de Simcoe Nord Muskoka. Il vise à planifier et à mettre en œuvre la solution cRGT. Cette solution bâtira la charpente requise pour fournir aux cliniciens un accès aux données sur leurs patients provenant de sources multiples, et ce, de manière fiable et sécurisée. Travaillant avec cyberSanté Ontario pour faire progresser la Stratégie ontarienne de cybersanté dans la région centrale de la province, le Réseau universitaire de santé (RUS) jouera le rôle de partenaire de prestation du programme.

La solution cRGT établira des liens électroniques entre les données sur les patients dans tout le continuum de soins et les intégrera afin de les rendre accessibles aux points de service pour appuyer la prestation de soins de santé et améliorer l'expérience des patients et des cliniciens. Cette information sur la santé inclura l'apport de services de données régionaux et provinciaux, y compris le Système d'information de laboratoire de l'Ontario (SILO), voire d'autres sources telles que le Programme de médicaments de l'Ontario et le Dépôt d'imagerie diagnostique de l'ouest de la région du Grand Toronto. La solution comprend deux composantes principales : une solution administrative permettant aux participants de transmettre et d'entreposer des RSP dans un dépôt de données cliniques (DDC), et une solution frontale permettant aux participants de voir les RSP du DDC sur les lieux des soins.

Le RUS projette de lancer une version de production limitée (VPL) de cRGT au quatrième trimestre de l'année financière 2013/14. Avec cette version limitée, environ 50 cliniciens de 16 organismes participant à cRGT pourront utiliser la solution cRGT et consulter les données cliniques de leurs patients.

La VPL sera mise en service en deux phases :

- Phase 1 : les cliniciens-utilisateurs finaux seront mis à contribution pour tester et valider la solution en milieu clinique afin de vérifier que les données cliniques sont fournies de manière à faciliter la prestation des soins;

- Phase 2 : les cliniciens-utilisateurs finaux profiteront de l'utilisation clinique générale de la solution.

En plus d'offrir aux cliniciens-utilisateurs finaux la possibilité de tester la solution cRGT, la VPL donnera au RUS la chance de mettre en pratique et de corriger le cadre opérationnel qui appuiera le programme cRGT, y compris le programme de protection de la vie privée et de sécurité.

Dans la VPL, la solution administrative cRGT soutiendra le peuplement du DDC par 16 participants initiaux, qui fourniront des RPS associés aux types de données prioritaires par messages HL7 (*Health Level* 7). Ces types de données seront uniquement les suivants :

- Documents et notes;
- Visites et rencontres;
- Résultats d'imagerie diagnostique;
- Autres résultats;
- Soins communautaires.

La VPL permettra également aux utilisateurs finaux de consulter les résultats d'analyses de laboratoire et de pathologie grâce à un flux de données provenant du SILO par l'intermédiaire de la solution frontale cRGT. Ces résultats serviront à la prestation des soins de santé des patients de ces utilisateurs. Chaque fois qu'un participant clinicien-utilisateur consulte des RPS au moyen de la solution, en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS), il est réputé avoir recueilli ces RPS en tant que dépositaire de renseignements sur la santé (DRS) des participants, qui ont fourni des RPS au DDC (et divulgué de ce fait ces RPS en tant que DRS).

La présente évaluation de l'impact sur la protection de la vie privée (ÉIPVP) a été menée par la firme MD+A Health Solutions pour le compte du RUS. Elle couvre les aspects suivants :

- L'ensemble du programme de protection de la vie privée et les mesures de protection des renseignements personnels de cRGT dans la mesure où la VPL est concernée;

- Les processus administratifs du programme cRGT qui incluent des RPS;

- Le droit du RUS, des participants à cRGT et des fournisseurs de services de participer à ces processus.

MD+A a en outre appliqué les dix principes du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation (CSA) dans son évaluation des mesures de protection de la vie privée et du programme que le RUS a mis en place pour protéger les RPS qui seront manipulés dans le cadre du programme et de la solution cRGT.

L'ÉIPVP n'a pas révélé de risques importants d'entrave à la vie privée. Le RUS a conçu un programme fiable de protection de la vie privée pour cRGT, qu'il est en train de mettre en œuvre. Ce programme comprend les éléments suivants :

- Une structure de gouvernance visant la protection de la vie privée et la sécurité;
- Un ensemble complet de politiques et de procédures visant la protection de la vie privée et la sécurité;
- Une équipe de protection de la vie privée et de sécurité chargée d'élaborer et de mettre en œuvre le programme de protection de la vie privée.

Les problèmes de protection de la vie privée et les risques qui ont été établis pour le RUS sont résumés à la section 1.1 ci-après. MD+A a relevé trois thèmes principaux relatifs aux risques recensés :

- Dix des dix-sept risques recensés concernent des composantes du programme de protection de la vie privée de cRGT qui sont incomplètes à l'heure actuelle, mais qui devraient être achevées avant le lancement de la VPL. Dans de nombreux cas, MD+A a eu la preuve substantielle que les

composantes sont presque terminées (p. ex., sous forme de documents préliminaires ou de présentations faites à des instances de gouvernance aux fins d'approbation d'une démarche politique).

- Le RUS a élaboré un ensemble complet de politiques de confidentialité et de sécurité afin d'orienter ses interactions avec les participants de cRGT lors d'opérations délicates, telles que les demandes d'accès ou la gestion des incidents. Les politiques et procédures ont été clairement énoncées par écrit et sont explicites quant aux mesures qui devraient être prises advenant certains scénarios très précis de protection de la vie privée.

  Cependant, il est possible que des participants à cRGT, ainsi que des patients, trouvent les politiques et procédures trop denses ou trop complexes pour être mises en œuvre comme l'entend le RUS. MD+A a recommandé une révision de la conformité aux politiques et des documents de communication à l'intention des patients, afin de présenter sans ambiguïté à ces derniers les options qui s'offrent à eux s'ils veulent se prévaloir de leurs droits en matière de protection de leurs renseignements personnels gérés par cRGT.

- Plusieurs inquiétudes soulevées par l'ÉIPVP concernent la relation du RUS avec les fournisseurs de services de cRGT, notamment TELUS (fournisseur des solutions frontale et administrative), et cyberSanté Ontario (fournisseur de services d'hébergement). Le RUS n'a pas encore établi de cadre d'opérations ou de vérification pour ses interactions avec ces fournisseurs pendant la durée d'utilisation de la VPL.

  Les participants de cRGT vont exiger de la clarté quant aux façons de traiter les RPS et aux activités des fournisseurs de services, si leur confiance dans les mesures de protection des renseignements personnels et de sécurité de cRGT doit être maintenue. Le RUS devrait s'assurer qu'il dispose d'un cadre avec lequel travailler et garantir le respect de la confidentialité et de la sécurité par les fournisseurs de services de cRGT.

MD+A recommande que le RUS élabore un plan de réaction aux risques pour répondre aux inquiétudes et pour appliquer les recommandations qui ont été formulées dans l'ÉIPVP, puis qu'il suive ce plan pour atténuer ou éliminer les risques recensés. Le RUS a créé un programme fiable de confidentialité et de sécurité pour l'initiative cRGT, et les auteurs de l'ÉIPVP croient que les problèmes relevés seront résolus par le RUS afin d'assurer le succès du lancement de la VPL.

Enfin, le RUS devrait envisager une évaluation supplémentaire de la protection de la vie privée entre le lancement de la VPL et la mise en service de la solution complète en milieu clinique.

1.1 Tableau des conclusions sur la protection de la vie privée

Risques pour la protection de la vie privée
1. L'accord de participation 4 (pour la période de visualisation) est incomplet.
2. Aucun processus n'a été établi pour permettre au comité sur la confidentialité et la sécurité de vérifier la non-conformité aux politiques de confidentialité de cRGT.

3. Il n'existe pas de procédure de conservation et de destruction des RPS recueillis par le RUS pour appuyer la mise en œuvre des procédures de confidentialité de cRGT.
4. Les politiques de protection de la vie privée peuvent être difficiles à appliquer à cause de leur complexité et de la portée et de l'ampleur des responsabilités assignées au RUS.
5. Le manuel de protection des renseignements personnels et de sécurité de la VPL et la rédaction des procédures internes du RUS ne sont pas encore terminés.
6. Aucun cadre opérationnel de confidentialité et de sécurité n'a été élaboré pour les fournisseurs de services de cRGT.
7. Le plan de formation sur la confidentialité et la sécurité de la VPL n'est pas terminé.
8. Les critères d'audit et de surveillance des participants n'ont pas été définis dans la politique d'audit de cRGT.
9. Aucun cadre d'audit n'a été établi pour les fournisseurs de services de cRGT et les autres fournisseurs de services.
10. Les données du SILO qui ne sont pas masquées dans la solution cRGT peuvent être vues par l'ensemble du personnel des organismes participants qui ont outrepassé la directive de consentement sur les données.
11. L'écran *Patient Overview* (aperçu du patient) du portail fournisseur de cRGT peut révéler davantage de renseignements que les RPS expressément demandés par les utilisateurs finaux.
12. Le RUS n'a pas rédigé de document sur les personnes œuvrant pour cRGT qui auront accès aux RPS et leurs rôles.
13. Le RUS n'a pas achevé la politique de conservation des données de cRGT.
14. Les administrateurs chargés de la confidentialité qui se connectent aux portails de confidentialité ou de consentement ne disposent pas d'une authentification complète à deux facteurs.
15. Le RUS ne saura pas si les organismes participants contrôlent correctement l'accès aux RPS offert par cRGT.
16. Le RUS n'a pas achevé le programme de vérification et d'assurance (en cours) qui peut garantir à chaque participant que les autres participants se plient aux exigences de confidentialité et de sécurité.
17. Le RUS n'a pas préparé de documents de communication pour encadrer les échanges avec les patients pendant les opérations engageant leurs renseignements personnels.

Conclusion

Le RUS a notablement progressé dans l'élaboration du programme de protection de la vie privée du projet cRGT et dans la conception des mesures de précaution qui étayent ce programme. Trois de ces mesures sont à souligner : une fonction de gouvernance fiable pour la protection de la vie privée – qui fournit à l'équipe de protection de la vie privée de cRGT et aux intervenants du projet des orientations et des apports adéquats –, un ensemble d'accords structurant et des politiques et procédures de confidentialité détaillées – qui aideront tous les intervenants de cRGT à assumer leurs obligations de confidentialité respectives et qui témoignent du respect des droits des patients en matière de protection des renseignements personnels.

La firme MD+A ne perçoit pas de problèmes majeurs dans les mesures de sécurité des renseignements et de sécurité technique qui ont été déployées pour la solution cRGT. L'équipe de protection de la vie privée de cRGT est bien intégrée avec les fonctions administratives de cRGT au sein du RUS – fonctions qui comprennent également la formation et l'adoption, ainsi que la mise en œuvre sur les lieux des soins – et les fonctions de planification opérationnelle de cRGT. Par conséquent, l'équipe bénéficie du soutien requis pour élaborer et mettre en œuvre le programme de protection de la vie privée de cRGT.

MD+A croit donc que le RUS est correctement positionné pour résoudre les problèmes de confidentialité qui ont été relevés par l'ÉIPVP, particulièrement les lacunes du programme de protection de la vie privée et de sécurité, que le RUS souhaite combler en vue de la VPL. Les principaux domaines dans lesquels le RUS devrait concentrer ses efforts avant le lancement de la VPL sont l'achèvement d'un plan de formation sur la confidentialité et la sécurité pour la VPL, un cadre opérationnel pour la collaboration du RUS et des fournisseurs de services de cRGT en ce qui concerne les activités engageant des renseignements personnels et la sécurité, le manuel de protection des renseignements personnels et de sécurité de la VPL et les critères d'audit et de surveillance étayant les politiques et procédures d'audit.

Des recommandations visant à résoudre les problèmes soulevés ont été émises. Dans de nombreux cas, il est simplement recommandé que le RUS mette la dernière main à la composante du programme de protection de la vie privée qui est analysée. Le RUS devrait toutefois élaborer un plan de réaction aux risques basé sur le registre des risques de l'ÉIPVP, afin de déterminer la manière dont il maîtrisera les possibilités d'entrave à la protection des renseignements personnels.